[19]中华人民共和国国家知识产权局

[51]Int. Cl[7]
G06F 11/20

[12]发明专利申请公开说明书

[21]申请号 00809715.1

[43]公开日 2002年7月17日

[11]公开号 CN 1359493A

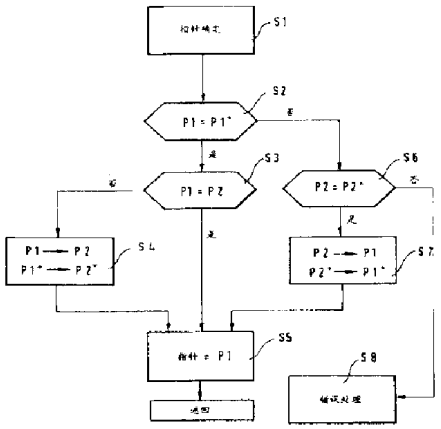
[22]申请日 2000.5.4 [21]申请号 00809715.1
[30]优先权
[32]1999.5.7 [33]DE [31]19921232.5
[86]国际申请 PCT/EP00/03990 2000.5.4
[87]国际公布 WO00/68794 德 2000.11.16
[85]进入国家阶段日期 2001.12.28
[71]申请人 德国捷德有限公司
地址 德国慕尼黑
[72]发明人 迪特尔·韦斯
[74]专利代理机构 北京市柳沈律师事务所
代理人 侯 宇 陶凤波

权利要求书2页 说明书6页 附图页数2页

[54]发明名称 用于安全写环形存储器指针的方法

[57]摘要

为使在一个循环存储器或环形存储器中,例如在EEPROM中,对 指向当前数据项的指针(P)的安全写成为可能,将向含有最陈旧数据项的 存储单元(R3)中写入新数据项(D'#3),然后将指针(P)修改。指针(P)由第一个指针(P1,P1*)和第二个指针(P2,P2*)构成,其中第二个指针是第一 个指针的冗余。每个指针含有一个测试值,它实际上是指针值的反码或 补码。通过第二个指针和测试值可以使指针得到最佳的安全写。如果在修改指针过程中发生故障,可以在之后选择是根据第二个指针的内容恢 复旧的第一个指针,还是借助于新的第一个指针将第二个指针也加以修 改。



ISSN1008-4274

01.12.28

权　利　要　求　书

1. 一种用于安全写指针(P)的方法，其中，指针指向环形存储器(10；10’)中被包含在存储单元(R1，R2，…)中的数据项，其中，

a） 除第一个指针(P1，P1*)，还额外增加一个与之冗余的第二个指针(P2，P2*)；而且

b） 对第一个指针以及第二个指针都扩充了一个测试值。

2. 根据权利要求 1 所述的方法，其特征在于，第一个指针(P1，P1*)和第二个指针(P2，P2*)是相互分开的，特别是在时间上是分开被写入的。

3. 根据权利要求 1 或 2 所述的方法，其特征在于，确定以及检查当前指针的步骤包括：

a） 根据测试值(P1*)检查第一个指针(P1)(S2)，

b） 将第一个指针与第二个指针进行比较(S3)，当第一个指针(P1)是正确的时候，

c） 根据步骤 b)，当两个指针相比较不一致时，拷贝第一个指针(到第二个指针)，以保证第二个指针是新的，

d） 当第一个指针(P1)不正确时，根据测试值(P2*)检查第二个指针(P2)(S6)，

e） 当根据步骤 d)检查得出第二个指针是正确的时候，用指针(P2，P2*)的值覆盖第一个指针(P1，P1*)(S7)。

4. 一种采用如权利要求 1 至 3 中任一项所述的方法来管理一个环形存储器(10；10’)的方法，其特征在于，为了将一个新数据项(D’#3)写入一个与由指针(P)指向的存储单元(R2)相连的指定存储单元(R3)中，将新数据项写入存储单元(R3)，然后修改指针。

5. 根据权利要求 4 所述的方法，其特征在于，在将新数据项(D’#3)写入指定的存储单元之前，要清除该单元的内容。

6. 根据权利要求 4 或 5 所述的方法，其特征在于，所述指定的存储单元含有环形存储器(10')中最陈旧的数据项，并且作为写缓冲器使用。

7. 根据权利要求 1 至 6 中任一项所述的方法，其特征在于，每个指针由相应的存储单元的地址码，以及其所属的用作测试值的该地址码的补码构成。

8. 一种具有确定数目存储单元(R1，...Rn)的环形存储器，其每个存储单元含有一个数据项(D#1，...)，它还具有指针存储单元，其中写有指针值，该指针指向含有当前数据项(D#2)的存储单元，其特征在于，第一个指针存储单元(RP1)用于存放第一个指针(P1，P1*)包括测试值(P1*)，第二个指针存储单元用于存放相对于第一个指针冗余的第二个指针(P2，P2*)包括测试值(P2*)。

9. 根据权利要求 8 所述的方法，环形存储器被用在如权利要求 1 至 7 中任一项所述的方法中。

10. 一种具有如权利要求 8 或 9 所述的环形存储器的智能卡。

说　明　书

用于安全写环形存储器指针的方法

本发明涉及一种用于安全写环形存储器指针的方法，此外还涉及一种带有一个指针存储单元的环形存储器，以及含有这样的环形存储器的智能卡(Chipkarte)。

环形存储器或称周期性存储器，其内容也被看作是周期性数据或相似的东西，它们可以是虚拟存储器或硬件存储器。环形存储器尤其是电子可擦洗的、可编程的固定存储器(EEPROM)的一种典型组织形式。本发明以及本发明的实施例特别涉及到这种固定存储器，尽管本发明可普遍适用于各种环形存储器。

一个环形存储器含有一定数量的存储单元，环形存储器中的周期性数据包含一系列数据项(记录)，每一个数据项存放在一个存储单元中。数据项被周期性地按顺序写入环形存储器，方法是，写入的新数据项将最陈旧的数据项覆盖。环形存储器的存储单元按升序 1，2，...n 连续编号，存储单元“1”周期性地与存储单元“n”相接。“当前”或最新数据项存放在由指针指示的一个存储单元中。在写入序列数据项时，指针将每次周期性地指向更高一个地址。

为了阐明本发明所涉及到的基本问题，在这里对向一个 EEPROM 结构的环形存储器中的一个指定的存储单元写入新数据项的过程作一详细描述。这种 EEPROM 尤其常用在智能卡中，因此此处的问题也主要与智能卡有关。

为了将一个新数据项写入一个指定的存储单元，而该存储单元中存有环形存储器中最陈旧的数据项，在新数据被写入之前，须将该单元中的旧数据清除。用通常的方法实现这些的步骤是，每次使指针指向更高一个地址，然后写入新的数据项。当掉电使写过程中断时，就有可能使新的数据项丢失，此外还有可能丢失指针信息，这是更重要的，指针信息的丢失使要存入下一个数据项的位置无法被确认。另一个问题是，指针的信息有可能是错误的信息，如在指针被修改后。

在现有技术中，对避免环形存储器的这类错误有许多建议。在 FR-A-2 699 704 中描述了一种修改 EEPROM 中数据的方案，在这个方案中设置了一个

多位的标志，每个标志相对于一个数据项。如果在标志为“旧”的数据项处需要写进新数据项时，首先要将该数据项以及它的标志清除，新数据项方可写入该旧数据项的位置，与之相关的标志将被赋值，这个值表明刚刚有数据修改发生。

然后到目前为止被标为当前数据项的标志将被改成“旧”的，新数据项的标志在操作的过程中被置为“当前”的。这种方法需要消耗一些操作和存储空间。如果在存入新数据项后，修改标志时出现中断，就会找不到新数据项，处于一种不确定状态。

从 EP-A-0 398 545 我们知道一种环形存储器，其中对于每一个数据项有一位标志位。当向环形存储器写入一个新的数据项时，在写过程之后跟随一个用表示当前数据的标志，如“1”来标记新数据项的过程。随后将把上一次是当前数据项的标志从“1”改为“0”。这样在这个过程中就有两个标志位同时为“1”。这种对于当前数据项的不确定的指针标志的混乱情况可以借助于约定来避免，当不止一个标志位为“1”时，总是“较高”的那位有效。由于一位的标志非常容易发生写错误，因此在修改指针标志位时极易产生错误的指针数据。

从 DE-A-196 50 993 我们知道一种环形存储器，它附加了一个在环形存储器接口之外看不到的存储单元。在写过程中，总是将最陈旧的数据项覆盖，随后，指针将这样被修改，即使其指向新的数据项。当发生故障时，只有最陈旧的数据项的信息被丢失，但这在接口之外是看不到的。这种存储系统也存在着这样的可能性，即由于对指针的误写而造成错误的指针信息。

本发明的目的在于，提供一种使安全写指针成为可能的方法。此外还提供了一种带有安全指针的环形存储器。

为实现本发明的目的，根据权利要求 1，不仅使用一个指针，还追加另一个冗余的指针。一种特别优选的实施形式是，第一个和第二个、冗余的指针要分开来写，特别是在时间上要分开，这样当写数据过程中发生可能的故障时，两个指针中至少有一个含有正确的指针信息。本发明的另一个特征是，第一个和第二个指针分别含有一个测试值。根据这些测试值可以区别出错误指针。可以仅仅通过一个写过程进行校正，亦即通过拷贝正确的指针来校正。

修改指针的第一步优选在建立第一个指针的测试值的同时进行。在将第一个、新的指针与第二个指针比较之后，在必要时将第一个指针拷贝到第二

个指针。

如果在写第一个和第二个指针时发生故障，如在写 EEPROM 时掉电，此时第一个指针可能已经被修改，而第二个指针中还是旧的值。根据故障发生的时间以及错误的类型可以或者根据第二个指针将第一个指针的原始信息恢复，或者按照第一个指针补加修改第二个指针。

尤其当两个指针在时间上分开写时，使用一个额外的、冗余的指针，可以实现能克服错误的指针数据的安全保护。此外由此带来的可能性是，在各种情况下都可以按需要重构指针内容，特别是当在修改指针过程中发生掉电时。每个指针所属的测试值主要由相关存储地址的补码构成。指针由当前存储单元的地址或称序号构成，测试值由其补码构成。

有一种特殊的结构，其中每个指针由两个字节组成，第一个字节(8 位)中含有地址码的两个 16 进制数，第二个字节含有该 16 进制数的补码。

根据本发明，通过一种值得推荐的方法，也可以实现多重冗余，以实际地在任意时间实现错误识别和错误校正。特别是当掉电发生时，使指针内容的重构成为可能。

根据本发明的方法，增加第二个指针以及测试值所消耗的存储空间以及额外的写周期是很有限的，但却实现了近乎完美的数据安全。这种优点尤其是在智能卡的应用中十分明显，在智能卡中含有敏感数据，对安全有特殊的需求。

与上述措施相关，该措施的另一项应用是，在周期性存储器中扩展一个存储单元，而这个额外的存储单元从外面，亦即环形存储器的接口之外，是看不到的。每次要被写入的新数据将被写入最陈旧的数据项的位置，这样当故障发生时，只有最陈旧的数据项会丢失，而这对外是不可见的，因为从外面只能看到不带额外存储单元的特定数目的存储单元。

下面依据附图对本发明的实施例进行详细描述。其中：

图 1 示出了一个环形存储器的第一个和第二个指针的存储单元；

图 2 为一个具有确定数量存储单元的环形存储器的示图，其中形象地示出了写入一个新数据项的三个阶段，以及相应的第一个和第二个指针的存储单元；

图 3 是一个流程图，它示出了第一个指针和第二个指针的修改过程以及奇偶校验，以及

图 4 是写第一个和第二个指针的三个相连接的步骤。

在下面要叙述的实施例中特别涉及到一种带有环形存储器管理的 EEPROM。为了向环形存储器中写入新的数据项，将以熟知的方式向 EEPROM 发送电信号，以改变指针指向的存储单元的状态。但是本发明也可以用于其他的环形存储器，也可以用于虚拟环形存储器。

先来看图 2，左边有一个标记着 I 的环形存储器 10，I 表示写过程的第一阶段。

环形存储器 10 有 n 个存储单元 R1，R2，R3，...Rn。在每一个存储单元中都有一个数据项，在图中用与编号存储单元相对的 D#1，D#2，...D#n 来表示。指针 P 指向当前的，在循环写过程中最新的数据，在本例中，在图 2 中 I，指针指向存储单元 R2 中的数据项 D#2。

在图 2 中环形存储器 10 的下方示出了指针 P。指针 P 含有第一个指针，它被存放在第一个指针存储单元 RP1，此外还有一个冗余的第二个指针，它被存放在另一个指针存储单元 RP2。

第一个指针实际上由指针元素构成，以存储单元地址码的形式出现，在这里用 P1 表示。第一个指针的其他组成部分是测试值，这里是作为 P1 补码的 P1*。第二个指针由第一个指针的拷贝构成，即 P2 也是由存储单元的地址码构成，而 P2*是 P2 的补码。

在本实施例中存储单元的地址由两个 16 进制代码组成。P1 的值为“02”，与其相应的补码为 FD(0，1，2，3，...9，A，B，C，D，F 的 16 进制补码为 F，E，D，3，2，1 以及 0)。图 1 展示了指针 P 的在两个存储位置 RP1 和 RP2 中的字节结构。第一个指针存储单元包含两个字节 b1 和 b2，其中 b1 是 b2 的补码，反之亦然。第二个指针存储单元 RP2 包含两个字节 b3 和 b4，这里他们的关系仍然是，b3，b4 互为补码。

根据图 2 所示的三个阶段 I，II，III，下面对如何将新数据项写到最陈旧的数据项的位置进行描述。在图 2 的左边展示出指针 P 指向存储单元 R2，该存储单元中的数据项为 D#2。根据环形存储器 10 的循环结构，按照定义，最陈旧的数据项应被包含在相邻的存储单元 R3 中。该单元中的数据项 D#3 应该被覆盖。这里首先将 R3 中的内容清除，然后将新数据项 D’#3 写入，如图 2 中间 II 所示。在写新数据项 D’#3 的过程结束之后，指针 P 将被修改，以指向最新的当前数据项 D’#3，如图 2 右边 III 所示。

在图 2 右下方展示了第一个指针和第二个指针的存储单元。如图所示，第一个指针(P1=03；P1*=FC)指向环形存储器的第三个存储单元 R3。

在图 2 的右边，环形存储器被标为 10'，用以说明本发明中一种特殊的结构形式。按照这种特殊的结构形式，环形存储器 10' 相对于图 2 所示的其他环形存储器版本增加了一个扩展的存储单元，它共含有 R(n+1)个存储单元。但是从环形存储器的接口外面看去，环形存储器 10' 仍然和从前一样只含有 n 个存储单元。这样在图 2 右边，下一次要写入数据项的存储单元是 R4，它含有作为写缓冲的数据项，即最陈旧的数据项，它从环形存储器之外不可读。在如上所述的写过程中，新数据项将被写入该存储单元。在发生故障的情况下，只有这个作为最陈旧数据项的冗余数据被丢失。

如图 2 下方所示的指针，它们是第一个指针 P1，P1*，第二个指针 P2，P2*，指针的修改发生在最新数据项，即图 2 中间所示的数据项 D' #3，被成功地写入之后。

如果在写指针，亦即在修改指针时发生故障，特别是发生掉电，则可以选择重构老的或新的指针。这一点如图 4 所示。

图 4 完整地展示了修改指针的三个阶段。在阶段“1”，指针处于旧状态。在阶段“2”，第一个指针 P1，P1*已经指向下一个地址，其内容为“03”和“FC”。在这一阶段，第二个指针的内容仍然是以前的值。在阶段“3”，第一个指针 P1，P1*的内容被拷贝到第二个指针中。

如果在阶段“2”发生故障，则第二个指针可以根据第一个指针 P1，P1*被确定为新的第二个指针，或者可以根据第二个指针将旧的第一个指针恢复。

图 3 根据流程图说明了确定当前指针值及其正确性检查的方法。确定/检查起始于步骤 S1。

在随后的步骤 S2 将检查指针 P1 是否与其测试值，这里即它的补码 P1*相一致。如果一致，将在步骤 S3 将第一个指针与第二个指针进行比较；如果不一致，则在步骤 S4 将第一个指针完整地拷贝到第二个指针中。

在步骤 S4 之后的步骤 S5，循环指针，也就是实际上对相应的存储单元起到寻址作用的指针，被设为 P1。如果在步骤 S3 的比较结果为两个指针 P1 和 P2 一致，则循环指针也在这里被设为 P 1 。

如果在步骤 S2 比较时发生奇偶错，则将在步骤 S6 对第二个指针做奇

偶检查。如果第二个指针 P2，P2*的奇偶性得到满足，则在步骤 S7 对第一个指针进行修正，即将第二个指针 P2 连同测试值 P2*一起拷贝到第一个指针中。这之后 P1 将再次用于相关存储单元的寻址。

如果在步骤 S6 中确定，第二个指针 P2 的值也不正确，则将在步骤 S8 中启动错误处理程序。

上述用于确定和检查分别含有作为测试值的补码或反码的第一个指针值和第二个指针值的方法，可结合图 2 简略示出的环形存储器 10 优选地以 EEPROM 的形式应用于智能卡中。

说　明　书　附　图

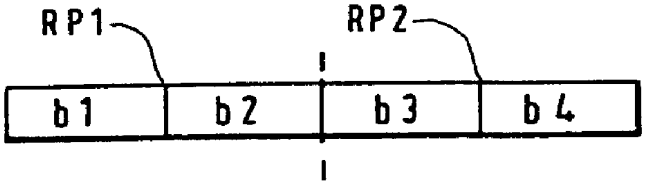


图 1

$b1 = \overline{b2}$

$b3 = \overline{b4}$

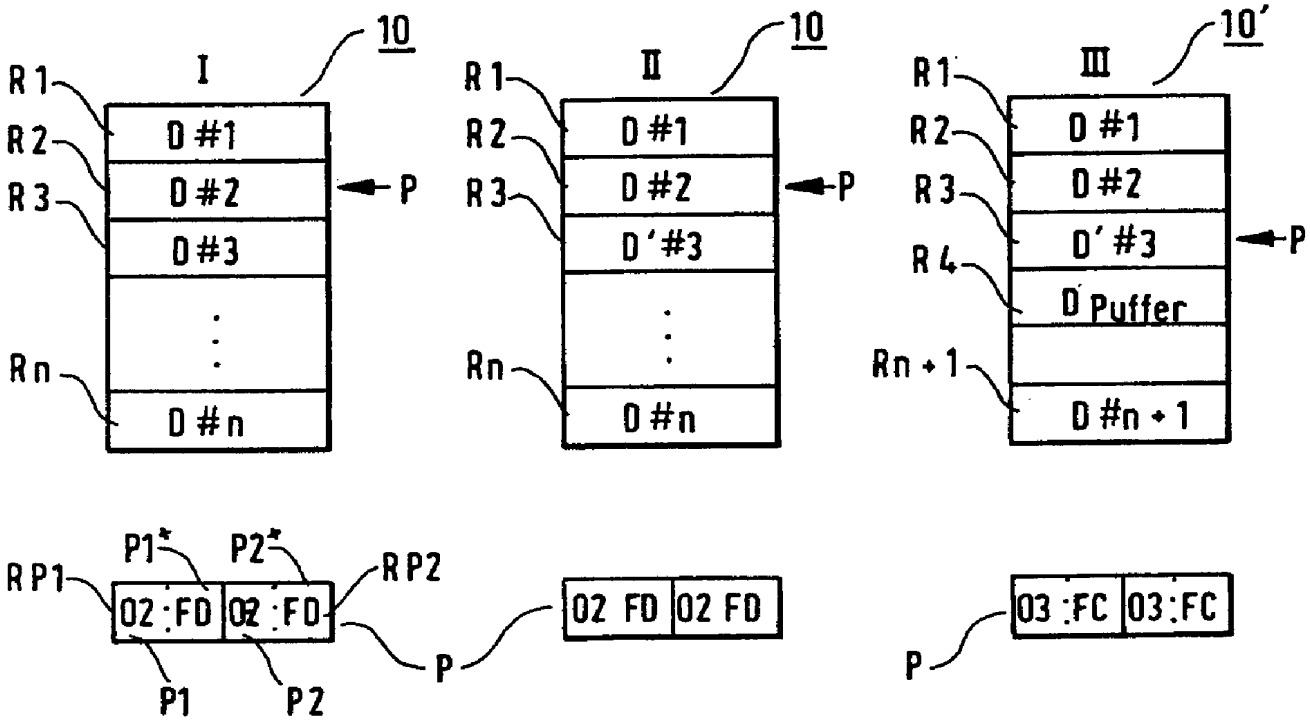


图 2

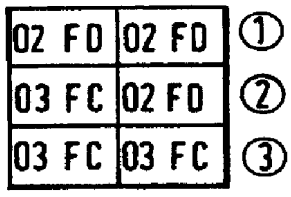


图 4

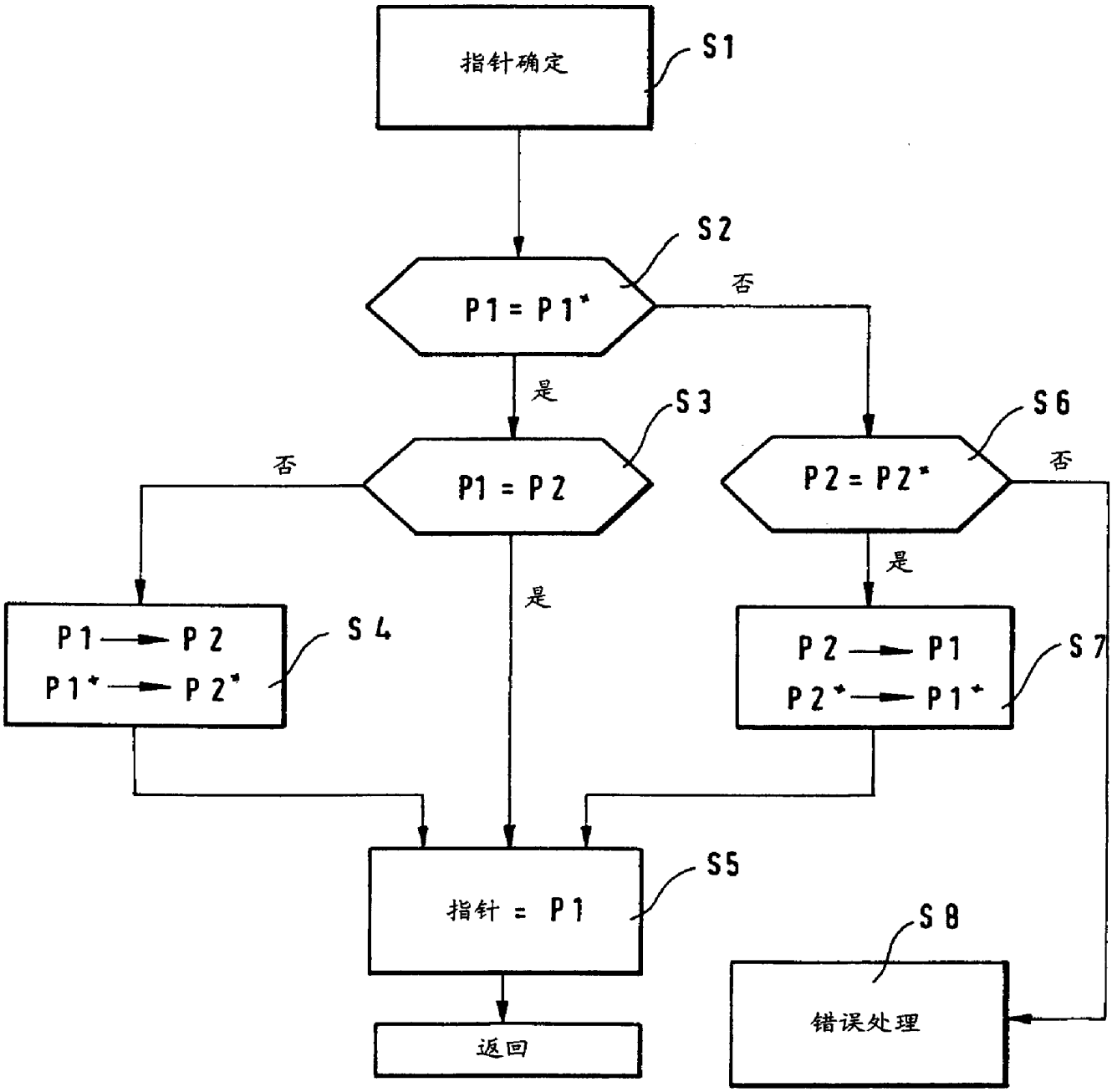

指针确定
S1
P1 = P1*
S2
否
是
P1 = P2
S3
否
是
P2 = P2*
S6
否
是
P1 → P2
P1* → P2*
S4
P2 → P1
P2* → P1*
S7
指针 = P1
S5
返回
S8
错误处理

图 3

Process for the secure writing of a pointer for a circular memory

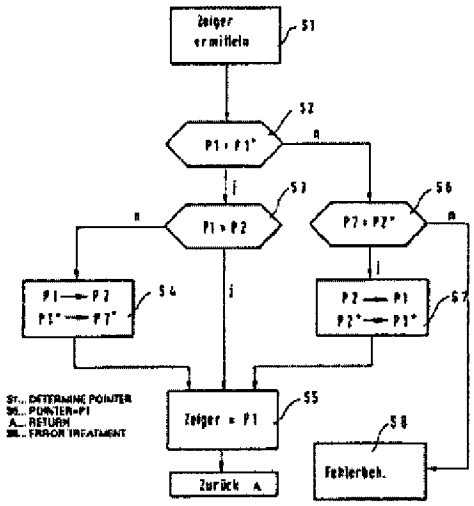
Publication number: CN1359493
Publication date: 2002-07-17
Inventor: WEISS DIETER (DE)
Applicant: GLESECKE & DEVRIENT GMBH (DE)
Classification:
- international: ***G06F12/16; G06F5/10; G11C16/02; G11C16/10; G11C29/04;*** **G06F12/16; G06F5/06; G11C16/02; G11C16/06; G11C29/04;** (IPC1-7): G06F11/20
- European: G06F5/10; G11C16/10E
Application number: CN20008009715 20000504
Priority number(s): DE19991021232 19990507

Also published as:
WO0068794 (A1)
EP1190324 (A1)
US6622205 (B1)
EP1190324 (A0)
DE19921232 (A1)
more >>

Report a data error here

Abstract not available for CN1359493
Abstract of corresponding document: **DE19921232**

The aim of the invention is to facilitate a secure writing of a pointer (P) that points to the respective actual data set in a cyclic memory or a circular memory such as an EEPROM. To this end, the new data set (D'#3) is written into the memory location (R3) that contains the oldest data set and the pointer (P) is updated. The pointer (P) consists of a first pointer (P1, P1*) and a second pointer (P2, P2*) that is redundant with respect to the first pointer. Every pointer contains a test value in the form of the inverse or complementary code of the proper pointer. The second pointer and the test value facilitate the writing of the pointer with an optimum of security. If an error occurs during the updating of the pointer, the previous first pointer can be optionally retrieved from the second pointer or the second pointer can be updated on the basis of the new first pointer.



Data supplied from the ***esp@cenet*** database - Worldwide